(11). Popovic R.S. va boshqalar (1983). “Dual-collector magnetotransistor optimized with respect to injection modulation.” Sensors and Actuators, 4, p. 155–163.

(12). Roumenin Ch.S. (1990). “Bipolar magnetotransistor sensors. An invited review.” Sensors and Actuators A: Physical, 24(2), p. 83–105.

(13). Castagnetti R., Wachutka G., Riccobene C., Baltes H. (1994). “Bipolar magnetotransistor: Relative sensitivity revisited.” ESSDERC 1994, p. 71–74.

(14). Trujillo H., Rodriguez F., Cruz J.C. (1996). “An approach to the electrical modelling of bipolar magnetotransistors.” Sensors and Actuators A: Physical, 56(3), p. 221–225.

(15). Trujillo H. va boshqalar (1995). “Merged lateral bipolar magnetotransistors.” Sensors and Actuators A: Physical, 50(3), p. 177–181.

(16). Nagy A., Trujillo H. (1998). “Highly sensitive magnetotransistor with new topology.” Sensors and Actuators A: Physical, 65(2–3), p. 97–100.

Ismailov Islombek Ilxombek o‘g‘li (Abu Rayhon Beruniy nomidagi Urganch davlat universiteti “Matematik tahlil” kafedrasi o‘qituvchisi; islombekursu@gmail.com),
Qurbanov Kamron Sanjar o‘g‘li (Abu Rayhon Beruniy nomidagi Urganch davlat universiteti “Matematik tahlil” kafedrasi o‘qituvchisi; kamron_kurbanov@mail.ru),
Sotimboyeva Zarina Ollabergan qizi (Abu Rayhon Beruniy nomidagi Urganch davlat universiteti Fizika-matematika fakulteti talabasi; zarinaursu@gmail.com)

EYLER FUNKSIYASI YORDAMIDA YECHILADIGAN NOSTANDART MASALALAR HAQIDA

Annotatsiya. *Ushbu maqolada sonlar nazariyasining fundamental va amaliy tushunchalaridan biri bo‘lgan Eyler funksiyasi, uning asosiy xossalari hamda algebraik, kombinatorik va olimpiada xarakteridagi nostandart masalalarni yechishdagi o‘rni va tatbiqlari keng atrofda tadqiq qilingan. Maqolada Eyler funksiyasining multiplikativlik xossasi, u bilan bog‘liq teoremalar (Eyler va Fermaning kichik teoremalari) va lemmalarning nazariy isbotlari keltirilgan. Shuningdek, yuqori darajali ko‘rsatkichli taqqoslamalarni yechish, sonlarning oxirgi raqamlarini hamda qoldiqlarni aniqlash, egizak tub sonlar va murakkab sonlar uchun tengsizliklarni isbotlashga doir murakkab va nostandart masalalarni sodda hamda samarali usullar yordamida yechish modellari ishlab chiqilgan. Maqola yakunida amaliy va mantiqiy tafakkurni rivojlantirishga qaratilgan mustaqil yechish uchun oliy darajali masalalar to‘plami taklif etilgan.*

Kalit so‘zlar: *tub sonlar, murakkab son, Eyler funksiyasi, Fermaning kichik teoremasi.*

О НЕСТАНДАРТНЫХ ЗАДАЧАХ, РЕШАЕМЫХ С ПОМОЩЬЮ ФУНКЦИИ ЭЙЛЕРА

Аннотация. *В данной статье подробно исследована функция Эйлера, являющаяся одним из фундаментальных и прикладных понятий теории чисел, а также ее свойства и применение при решении нестандартных, алгебраических и олимпиадных задач. В работе приведены теоретические доказательства свойства мультипликативности функции Эйлера, ключевых лемм и теорем (теоремы Эйлера и малой теоремы Ферма). Разработаны эффективные и упрощенные модели решения сложных задач, связанных с нахождением остатков от деления, определением последних цифр высоких степеней чисел, а также доказательством неравенств для составных и парных простых чисел. В заключительной части статьи представлен комплекс задач для самостоятельного решения, направленный на развитие логического мышления и исследовательских навыков учащихся.*

Ключевые слова: *простые числа, составные числа, функция Эйлера, малая теорема Ферма.*

ON NON-STANDARD PROBLEMS SOLVED USING EULER’S TOTIENT FUNCTION

Annotation. *This paper presents a comprehensive study of Euler's totient function, one of the fundamental concepts in number theory with significant theoretical and practical applications. The work explores the key mathematical properties of Euler's function, including its multiplicativity, alongside rigorous theoretical proofs of related lemmas and core theorems, such as Euler's theorem and Fermat's Little Theorem. Efficient methodologies and algorithmic models are proposed to solve non-standard, high-level contest problems involving modular exponentiation, remainder evaluation, determination of trailing digits, and inequality proofs for prime and composite numbers. Furthermore, a curated set of advanced problems is provided for independent study to enhance analytical problem-solving and algorithmic thinking.*

Key words. *Prime numbers, composite numbers, Euler's totient function, Fermat's little theorem.*

Kirish. Zamonaviy matematika, axborot xavfsizligi va kriptografiya sohalarining jadal rivojlanishi sonlar nazariyasining fundamental tushunchalariga bo‘lgan talabni yanada oshirmoqda. Ana shunday mu-

him va keng qamrovli tushunchalardan biri Eyler funksiyasidir ($\varphi(n)$). Matematika tarixida Leonard Eyler tomonidan kiritilgan ushbu funksiya nafaqat nazariy ahamiyatga ega, balki bugungi kunda raqamli ma'lumotlarni shifrlash (masalan, RSA algoritmi) va kompyuter ilmlarida amaliy jihatdan cheksiz imkoniyatlarni ochib bermoqda. Oliy ta'lim muassasalarining fundamental matematika va amaliy matematika yo'nalishlarida ushbu mavzuni chuqur o'rganish talabalarning mantiqiy va algoritmlash tafakkurini shakllantirishda muhim poydevor bo'lib xizmat qiladi. Odatda, o'quv dasturlarida Eyler funksiyasi va uning xossalari standart formulalar hamda oddiy misollar (masalan, berilgan sonning Eyler funksiyasini hisoblash yoki oddiy taqqoslamalarni yechish) doirasida cheklanib qoladi. Biroq nufuzli xalqaro olimpiadalar (IMC, Putnam va boshqalar) hamda chuqurlashtirilgan ilmiy tadqiqotlarda ayni shu funksiya yordamida yechila-digan, yuqori tartibli mantiq va nostandart yondashuv talab qiladigan murakkab masalalar tez-tez ko'zga tashlanadi. Bunday nostandart masalalarni yechishda talabalar va yosh tadqiqotchilar standart qoliplardan chiqib ketish, funksiyaning tub va murakkab sonlar bilan bog'liqlik xossalarini o'zaro integratsiya qilish prinsiplarida qiyinchiliklarga duch kelishadi.

Mavzuga oid adabiyotlarning tahlili va tadqiqot metodologiyasi. Sonlar nazariyasi matematikaning eng qadimgi va fundamental tarmoqlaridan biri bo'lib, Eyler funksiyasi va uning xossalari asrlar davomida ko'plab xorijiy va mahalliy olimlarning tadqiqot obyekti bo'lib kelgan.

Xalqaro miqyosda G.Hardy va E.Wright [3] o'zlarining fundamental asarlarida Eyler funksiyasining ($\varphi(n)$) multiplikativlik xossalarini va uning tub sonlar taqsimoti bilan bog'liqligini chuqur tahlil qilganlar. D.Burton [4] va K.Rosen [5] kabi olimlar esa darsliklarida ushbu funksiyaning elementar va amaliy jihatlarini, xususan, chiziqli taqqoslamalar tizimini yechishdagi rolini tizimlashtirganlar. Koblitz [10] o'z tadqiqotlarida Eyler teoremasining zamonaviy asimmetrik kriptotizimlarda (RSA algoritmi) qo'llanilishi, ya'ni, ochiq kalitli shifrlashning matematik asosi aynan shu funksiyaning hisoblash qiyinchiliklariga asoslanishini ilmiy jihatdan ko'rsatib bergan.

Mahalliy matematik olimlardan S.Sirojiddinov [8], N.Aleyev va Sh.Tojiyev [1] o'z o'quv qo'llanmalarida Eyler funksiyasi va Fermaning kichik teoremasini oliy ta'lim dasturlariga moslashtirilgan holda bayon etganlar. A.Asqarov [2] esa olimpiada matematikasida sonlar nazariyasining o'rnini yoritib, Eyler funksiyasiga doir ayrim nostandart kombinatorik va algebraik muammolarni hal qilish usullarini ko'rib chiqqan.

Biroq mavjud adabiyotlar tahlili shuni ko'rsatadiki, aksariyat manbalarda ushbu mavzu yo sof akademik teoremalar isboti shaklida yoki standart algoritmlar doirasida yoritilgan. Eyler funksiyasi yordamida yechiladigan oliy tartibli, nostandart va murakkab masalalarni yagona bir tizimga keltirish va ularning soddalashtirilgan yechim modellarini yaratish masalasi hamon dolzarb bo'lib qolmoqda.

Tahlil va natijalar. **Ta'rif.** n dan kichik musbat butun sonlar ichida n soni bilan o'zaro tub sonlarning soni $\varphi(n)$ bilan belgilanadi.

P1: $\varphi(10) = ?$ $(10;1);(10;3);(10;7);(10;9)$, demak, 10 dan kichik musbat butun sonlar ichida 10 soni bilan o'zaro tub sonlarning soni jami 4 ta bo'ladi.

1-lemma. Agar p tub son bo'lsa, $\varphi(p) = p-1$ ga teng bo'ladi.

Isbot. Agar p – tub son bo'lsa, p dan kichik va u bilan o'zaro tub sonlar $p-1$ ta bo'ladi (p o'zi bilan o'zaro tub emas). 1 dan $p-1$ gacha bo'lgan sonlar p soni bilan o'zaro tub, ya'ni $\varphi(p) = p-1$. ▲

P2. Agar $p = 47 \Rightarrow \varphi(47) = 47-1 = 46$ ta bo'ladi.

1-teorema. Agar p –tub va α –butun musbat son bo'lsa, quyidagi o'rinli bo'ladi: $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ formula o'rinli bo'ladi.

Isboti. $n = p^\alpha$ belgilash kiritsak, $\varphi(n)$ni topamiz. Endi biz 1 dan $n$gacha bo'lgan natural sonlar ichida n bilan o'zaro tub sonlar sonini topamiz. n gacha bo'lgan sonlar ichida n ga karrali $\frac{p^\alpha}{p} = p^{\alpha-1}$ ta son bor, demak, $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ bo'ladi. ▲

P3. 1) $\varphi(32) = \varphi(2^5) = 2^5 - 2^4 = 16$, demak, $\varphi(32) = 16$ ga teng.

2), $\varphi(125) = \varphi(5^3) = 5^3 - 5^2 = 100$, demak, $\varphi(125) = 100$ ga teng.

2-teorema. Istalgan a va b o‘zaro tub sonlar uchun $\varphi(a\cdot b)=\varphi(a)\cdot\varphi(b)$ tenglik o‘rinli bo‘ladi. Agar a va b sonlari o‘zaro tub bo‘lmasa, ya’ni, $EKUB(a,b)=d\neq 1$ bo‘lsa, u holda $\varphi(a\cdot b)=\varphi(a)\cdot\varphi(b)\cdot\dfrac{d}{\varphi(d)}$ tenglik o‘rinli bo‘ladi.

Isboti. Ma’lumli, $\forall n$ soni uchun $\varphi(n)$ ni hisoblaymiz: n soni $n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot p_3^{\alpha_3}\cdot\ldots\cdot p_k^{\alpha_k}$ kabi tub ko‘paytuvchilarga ajralsin (p_i –tub son, $i=\overline{1,k}$). $\varphi(n)=\varphi(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k})=$

$=\varphi(p_1^{\alpha_1})\cdot\varphi(p_2^{\alpha_2})\cdot\ldots\cdot\varphi(p_k^{\alpha_k})$ $=(p_1^{\alpha_1}-p_1^{\alpha_1-1})\cdot(p_2^{\alpha_2}-p_2^{\alpha_2-1})\cdot\ldots\cdot(p_k^{\alpha_k}-p_k^{\alpha_k-1})=$

$=p_1^{\alpha_1}\left(1-p_1^{-1}\right)p_2^{\alpha_2}\left(1-p_2^{-1}\right)\ldots p_k^{\alpha_k}\left(1-p_k^{-1}\right)=$ $=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}\cdot\left(1-\dfrac{1}{p_1}\right)\left(1-\dfrac{1}{p_2}\right)\ldots\left(1-\dfrac{1}{p_k}\right)=$

$=n\cdot\left(1-\dfrac{1}{p_1}\right)\left(1-\dfrac{1}{p_2}\right)\ldots\left(1-\dfrac{1}{p_k}\right).$

Demak, $\varphi(n)=n\cdot\left(1-\dfrac{1}{p_1}\right)\left(1-\dfrac{1}{p_2}\right)\ldots\left(1-\dfrac{1}{p_k}\right)$ ▲

Bu formula *Eylerning umumlashgan funksiyasi* deyiladi.

P4. $\varphi(2025000)=?$ Demak, $n=2^3\cdot3^4\cdot5^5$ ga teng bo‘lgani uchun $\varphi(2^3\cdot3^4\cdot5^5)=$

$=2^3\cdot3^4\cdot5^5\cdot\left(1-\dfrac{1}{2}\right)\left(1-\dfrac{1}{3}\right)\left(1-\dfrac{1}{5}\right)=2^5\cdot3^3\cdot5^4$ ga tengligi kelib chiqadi.

P5. Agar n – musbat murakkab son bo‘lsa, quyidagi $\varphi(n)\le n-\sqrt{n}$ tengsizlikni isbotlang.

Isboti. n soni murakkab son bo‘lgani uchun, $n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}$ kabi tub ko‘paytuvchilarga ajralsi (p_i – tub son, $i=\overline{1,k}$). u holda $p_i\le\sqrt{n}$ shart o‘rinli bundan

$\varphi(n)=n\cdot\left(1-\dfrac{1}{p_1}\right)\left(1-\dfrac{1}{p_2}\right)\ldots\left(1-\dfrac{1}{p_k}\right)\le n\left(1-\dfrac{1}{p_i}\right)\le n\left(1-\dfrac{1}{\sqrt{n}}\right)=n-\sqrt{n}\Rightarrow\varphi(n)\le n-\sqrt{n}$ ▲

ekani kelib chiqadi.

P6. $\forall n$ natural soni uchun $\varphi(n)\vdots10$ shartni qanoatlantiruvchi cheksiz sonlar borligini isbotlang.

Isboti. $n=11^k$, k = 1, 2, 3, ... bo‘lsa, $\varphi(11^k)=11^k-11^{k-1}$ bundan esa $\varphi(11^k)=11^{k-1}(11-1)=10\cdot11^{k-1}\Rightarrow\varphi(11^k)=10\cdot11^{k-1}\vdots10$, $k\in\mathbb{N}$ sonlar cheksiz ko‘p ekani kelib chiqadi. Isbot tugadi.▲

P7. $p-1$ va $p+1$ lar egizak tub sonlar va $p>4$ bo‘lsa, p soni uchun $3\varphi(p)\le p$ tengsizlik o‘rinli bo‘ladi.

Isboti. Demak, $p-1$ va $p+1$ lar egizak tub sonlar va $p>4$ bo‘lsa, p soni 6 ga qoldiqsiz bo‘linadi. $p=2^a\cdot3^b\cdot m$, $a,b\ge1$ $EKUB(6,m)=1$ demak, $\varphi(2^a\cdot3^b\cdot m)=\varphi(2^a)\cdot\varphi(3^b)\cdot\varphi(m)$

$=(2^a-2^{a-1})\cdot(3^b-3^{b-1})\cdot\varphi(m)=$ $=2^a\cdot3^{b-1}\cdot\varphi(m)\le2^a\cdot3^{b-1}\cdot m=\dfrac{p}{3}$ $\Rightarrow\varphi(p)\le\dfrac{p}{3}\Rightarrow3\varphi(p)\le p$

tengsizlik kelib chiqadi. ▲

3-teorema. (Eyler teoremasi). $\forall\ a,m\in\mathbb{N}$. Agar $EKUB(a,m)=1$ bo‘lsa, $a^{\varphi(m)}\equiv1(\mathrm{mod}\,m)$ tenglik o‘rinli bo‘ladi.

Isboti. Quyidagi lemmadan foydalanamiz.

1-lemma. $\forall n\ a,m\in\mathbb{N}$. Agar (a,m) o‘zaro tub sonlar va m dan kichik va u bilan o‘zaro tub sonlar $r_1,r_2,\ldots,r_{\varphi(m)}$ bo‘lsa, $ar_1,ar_2,ar_3,\ldots,ar_{\varphi(m)}$ larni m ga bo‘lgandagi qoldiqlar har qaysi tartibda o‘rin almashgan $r_1,r_2,\ldots,r_{\varphi(m)}$ lar bilan bir xildir. Endi $(a,m)=1\Rightarrow$ lemmaga ko‘ra, $\Rightarrow$

$(ar_1)\cdot(ar_2)\cdot\ldots\cdot(ar_{\varphi(m)}) \equiv r_1\cdot r_2\cdot\ldots\cdot r_{\varphi(m)} \pmod m$

$a^{\varphi(m)}\cdot(r_1\cdot r_2\cdot r_3\ldots r_{\varphi(m)}) \equiv r_1\cdot r_2\cdot r_3\ldots r_{\varphi(m)} \pmod m$ va $(r_i,m)=1$ bo'lgani uchun

$(i\in\{1,2,\ldots,\varphi(m)\})$, $(r_1\cdot r_2\ldots r_{\varphi(m)},m)=1$ hamda $a^{\varphi(m)}\equiv 1\pmod m$ tenglik o'rinli bo'ladi.

Eslatma: Fermaning kichik teoremasining umumlashgan tenglamasi Eyler teoremasi bo'ladi.

4-teorema. (Fermaning kichik teoremasi). $\forall\, a,p\in\mathbb{N}$, p – tub son va $(a,p)=1$ bo'lsa, $a^{p-1}\equiv 1\pmod p$ tenglik o'rinli bo'ladi.

Isboti. $(a,p)=1$, $\varphi(p)=p-1$ va Eyler teoremasiga ko'ra,

$a^{\varphi(p)}\equiv 1 \pmod p$

$a^{p-1}\equiv 1 \pmod p$ kelib chiqadi. ▲

P8. 2^{98} ni 33ga bo'lgandagi qoldiqni toping.

Yechish. Biz Eyler umumlashgan teoremasini juda yaxshi bilamiz. $\varphi(33)=\varphi(3\cdot 11)=(3-1)(11-1)=20$ bundan esa $\varphi(33)=20$, $2^{\varphi(33)}\equiv 1 \pmod{33}$

$x=2^{98}\equiv 2^{100}\cdot 2^{-2}\equiv (2^{20})^5\cdot 2^{-2}\equiv 2^{-2} \pmod{33} \Rightarrow 4x\equiv 1 \pmod{33} \Rightarrow x\equiv 25 \pmod{33}$

demak, 25 qoldiq qoladi.

P9. $a_n=6^n+8^n$, $n\in\mathbb{N}$. a_{83} ni 49 ga bo'lgandagi qoldiqni toping.

Yechimi. $\varphi(49)=\varphi(7^2)=7^2-7=42$ shuning uchun $6^{84}\equiv 1 \pmod{49}$ $8^{84}\equiv 1$ (mod49) o'rinli bo'ladi. Endi $a_{83}=6^{83}+8^{83}\equiv 6^{84}\cdot 6^{-1}+8^{84}\cdot 8^{-1}\equiv$

$\equiv (6^{84})\cdot(6^{-1})+(8^{84})\cdot(8^{-1})\pmod{49} \equiv 6^{-1}+8^{-1}\pmod{49} \equiv (6+8)\cdot 6^{-1}\cdot 8^{-1}\pmod{49}\equiv$

$\equiv 14\cdot 48^{-1}\pmod{49}\equiv 14\cdot(-1)\pmod{49}\equiv -14\pmod{49}\equiv 35\pmod{49} \Rightarrow$ qoldiq 35 ga teng. **Izoh:** $48^{-1}\pmod{49}\equiv -1$ bo'ladi.

P10. 1032^{1032} ning oxirgi ikki raqamini toping.

Yechilishi. Demak, $n=1032^{1032}$ ning oxirgi ikki raqamini topish uchun n ni 100 ga bo'lgandagi qoldiqni topish yetarli bo'ladi. $100=4\cdot 25$

$1032^{1032}\equiv 0 \pmod 4$ (1)

$1032^{1032}\equiv (1032 \pmod{25})^{1032}\equiv$

$\equiv 7^{1032}\equiv(-1)^{516}\equiv 1 \pmod{25}$

$$\begin{cases} n=4a \\ n=25b+1 \end{cases} \Rightarrow n\equiv 76 \pmod{100}$$

demak, oxirgi 2 ta raqami 76 ga teng.

Mustaqil yechish uchun masalalar

P1. Ixtiyoriy n natural soni uchun $\varphi(3n)=3\varphi(n)$ tenglik o'rinli bo'lishi uchun n soni qanday shartni qanoatlantirishi kerak?

P2. $a_n=5^n+11^n$, $n\in\mathbb{N}$ ketma-ketlik berilgan. a_{41} hadini 36 ga bo'lgandagi qoldiqni aniqlang.

P3. Agar p va q turlicha tub sonlar bo'lsa, $p^{q-1}+q^{p-1}\equiv 1 \pmod{p\cdot q}$ quyidagi taqqoslamaning o'rinli ekanini isbotlang.

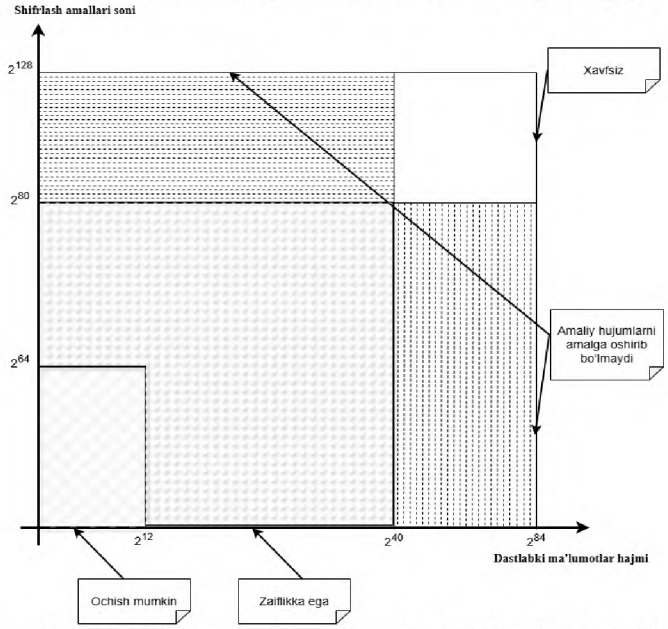
P4. Istalgan $n\in\mathbb{N}$ uchun $\varphi(n)+\sigma(n)\geq 2n$ tengsizlik o'rinli ekanini isbotlang (Bu yerda $\sigma(n)$ – n sonining barcha natural bo'luvchilari yig'indisi).

P5. (Putnam olimpiadasi). $\forall\, n>1$ bo'lganda, n soni $2^{n-1}-1$ sonini bo'lishi mumkinmi? P6. $\forall\, n\in\mathbb{N}$ uchun $n^2\mid\varphi(5^n-1)$ ekanini isbotlang.

Yopiq kalit uzunligi shifrning bardoshliligini baholashda muhim ahamiyatga ega. Kalit uzunligini oshirish hujumlarning ko‘p turlariga qarshi himoya qilishga yordam beradi. Shu bilan birga, kalitning ortiqcha uzunligi shifrlash tezligiga salbiy ta’sir ko‘rsatadi. Shu sababli tezkorlik va xavfsizlik o‘rtasidagi muvozanatni topish muhim hisoblanadi. So‘nggi yillarda kriptologiyaning barcha masalalari bo‘yicha ilmiy ishlarning juda jadal o‘sishini kuzatish mumkin. Jumladan, kriptologiyaning kriptotahlil yo‘nalishi juda izchillik bilan faol rivojlanayotgan tadqiqot sohasi hisoblanadi.

Kriptografik algoritmning bardoshliligi uni kriptotahlil uchun talab qilinadigan mehnat sarfi bilan belgilanadi. G‘araz niyatli tomonning intellektual va hisoblash imkoniyatlari turlicha bo‘lganligi sababli, shifrlash xavfsizligini ta’minlash uchun ishonchli chora-tadbirlar zarur. Kalit uzunligi, shifrlash tezligi va amalga oshirish qulayligi shifrlash tizimining samaradorligini baholashda muhim ahamiyatga ega [3;31–79-b.].

II. Mavzuga oid adabiyotlarning tahlili. Bugungi kunda zamonaviy EHM imkoniyatlari, talab etuvchi dastlabki ma’lumotlar va hisoblash resurslariga ko‘ra, ixtiyoriy kriptotahlil usulining amaliy ahamiyatini 1-rasmda tasvirlangan grafik asosida baholash mumkin [4;8–10-b.]. Shuni ham ta’kidlash lozimki, EHM imkoniyatlarining oshishi 1-rasmda tasvirlangan sohalar ko‘lamining kengayishiga ham olib keladi.



1-rasm. Turli kriptotahlil usullari amaliy qo‘llash imkoniyatlarini baholash.

Tarmoqlarda shifrlangan ma’lumotni uzatish jarayonida kriptotahlilchi: passiv yoki aktiv hujum turlarini amalga oshirishi mumkin [5;8–75-b.; 6;51–120-b.].

Passiv hujum maxfiy ma’lumotni aloqa tarmog‘ida uzatilayotganda eshitish, tahlil qilish, yozib olish kabi xatti-harakatlardan iborat bo‘lib, uzatilayotgan ma’lumot qabul qiluvchiga o‘zgarishsiz yetib boradi.

Aktiv hujum maxfiy ma’lumot uzatish jarayonini uzib qo‘yish, modifikatsiyalash, qalbaki shifr ma’lumotlar tayyorlash kabi xatti-harakatlardan iborat.

III. Tadqiqot metodologiyasi. Ishlab chiqilgan va [7;69–92-b.] adabiyotda to‘liq bayoni keltirilgan asimmetrik shifrlash algoritmi uchun quyidagi kriptohujum usullari ko‘rib chiqilishi mumkin:

Shifr matnga asoslangan hujumlar (Ciphertext-Only Attack). Bu usul kriptotahlil uchun eng kam ma’lumot sarfini tahlil qiladi: bunda shifrlangan ma’lumot ushlab olinadi va ochiq matnni, iloji bo‘lsa, yopiq kalitni topish ko‘zda tutiladi.

Ushbu usul eng murakkab hujum usullaridan biri hisoblansa-da, barcha zamonaviy kriptotizimlar, hech bo‘lmaganda, ushbu hujumni hisobga olgan holda ishlab chiqilgan bo‘lishi zarur [8;281–320-b.]. Agar al-goritm shifrlangan matnga asoslangan hujumga bardoshli bo‘lmasa, bu xabarlar yopiq kanallar orqali yu-borilishini anglatadi, bunday holda shifrlashga hojat qolmaydi.

Ma’lum ochiq matn asosidagi hujumlar (Known Plaintext Attacks). Ochiq va mos shifrlangan matn bloklari juftligi mavjud bo‘lgan holda algoritm tahlil qilinadi. Ma’lum bo‘lgan ochiq matn hujumi, hujumchiga shifrlangan matnni qo‘lga kiritganini va u bilan mos keladigan ochiq matnni bilishini va hujumchi yopiq kalitni olishni xohlayotganini bildiradi. Ma’lum bo‘lgan ochiq matn asosidagi hujum hali ham ko‘pchilik hollarda zarur hisoblanadi.